This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

JFW

PTO/SB/21 (08-03)
Approved for use through 08/30/2003. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	10/709,635
Filing Date	05/19/2004
First Named Inventor	Chih-Chung Lu
Art Unit	
Examiner Name	
Attorney Docket Number	IEIP0011USA

Total Number of Pages in This Submission: 3

ENCLOSURES *(Check all that apply)*

- [x] Fee Transmittal Form
  - [ ] Fee Attached
- [ ] Amendment/Reply
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [ ] Information Disclosure Statement
- [x] Certified Copy of Priority Document(s)
- [ ] Response to Missing Parts/ Incomplete Application
  - [ ] Response to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s) _____
- [ ] After Allowance communication to Technology Center (TC)
- [ ] Appeal Communication to Board of Appeals and Interferences
- [ ] Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- [ ] Proprietary Information
- [ ] Status Letter
- [ ] Other Enclosure(s) (please Identify below):

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm or Individual name	Winston Hsu, Reg. No.: 41,526
Signature	Winston Hsu
Date	5/27/2004

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below.

Typed or printed name			
Signature		Date	

PTO/SB/17 (10-03)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

FEE TRANSMITTAL for FY 2004

Effective 10/01/2003. Patent fees are subject to annual revision.

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 0.00

Complete if Known	
Application Number	10/709,635
Filing Date	05/19/2004
First Named Inventor	Chih-Chung Lu
Examiner Name	
Art Unit	
Attorney Docket No.	IEIP0011USA

METHOD OF PAYMENT *(check all that apply)*

☑ Check ☐ Credit card ☐ Money Order ☐ Other ☐ None

☑ Deposit Account:

Deposit Account Number: 50-3105

Deposit Account Name: North America Intellectual Property Corp.

The Director is authorized to: *(check all that apply)*

☑ Charge fee(s) indicated below ☐ Credit any overpayments

☑ Charge any additional fee(s) or any underpayment of fee(s)

☐ Charge fee(s) indicated below, **except for the filing fee** to the above-identified deposit account.

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1001	770	2001	385	Utility filing fee	
1002	340	2002	170	Design filing fee	
1003	530	2003	265	Plant filing fee	
1004	770	2004	385	Reissue filing fee	
1005	160	2005	80	Provisional filing fee	

SUBTOTAL (1) ($) 0.00

2. EXTRA CLAIM FEES FOR UTILITY AND REISSUE

	Extra Claims		Fee from below	Fee Paid
Total Claims		-20** =		X =
Independent Claims		- 3** =		X =
Multiple Dependent				=

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
1202	18	2202	9	Claims in excess of 20
1201	86	2201	43	Independent claims in excess of 3
1203	290	2203	145	Multiple dependent claim, if not paid
1204	86	2204	43	** Reissue independent claims over original patent
1205	18	2205	9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($) 0.00

***or number previously paid, if greater; For Reissues, see above*

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1051	130	2051	65	Surcharge - late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet	
1053	130	1053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for *ex parte* reexamination	
1804	920*	1804	920*	Requesting publication of SIR prior to Examiner action	
1805	1,840*	1805	1,840*	Requesting publication of SIR after Examiner action	
1251	110	2251	55	Extension for reply within first month	
1252	420	2252	210	Extension for reply within second month	
1253	950	2253	475	Extension for reply within third month	
1254	1,480	2254	740	Extension for reply within fourth month	
1255	2,010	2255	1,005	Extension for reply within fifth month	
1401	330	2401	165	Notice of Appeal	
1402	330	2402	165	Filing a brief in support of an appeal	
1403	290	2403	145	Request for oral hearing	
1451	1,510	1451	1,510	Petition to institute a public use proceeding	
1452	110	2452	55	Petition to revive - unavoidable	
1453	1,330	2453	665	Petition to revive - unintentional	
1501	1,330	2501	665	Utility issue fee (or reissue)	
1502	480	2502	240	Design issue fee	
1503	640	2503	320	Plant issue fee	
1460	130	1460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	
1809	770	2809	385	Filing a submission after final rejection (37 CFR 1.129(a))	
1810	770	2810	385	For each additional invention to be examined (37 CFR 1.129(b))	
1801	770	2801	385	Request for Continued Examination (RCE)	
1802	900	1802	900	Request for expedited examination of a design application	

Other fee (specify) _____

*Reduced by Basic Filing Fee Paid

SUBTOTAL (3) ($) 0.00

SUBMITTED BY				(Complete *(if applicable)*)	
Name (Print/Type)	Winston Hsu	*Registration No. (Attorney/Agent)*	41,526	*Telephone*	886289237350
Signature	Winston Hsu			*Date*	5/27/2004

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

This collection of information is required by 37 CFR 1.17 and 1.27. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/SB/02B (11-00)
Approved for use through 10/31/2002. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

DECLARATION — Supplemental Priority Data Sheet

Additional foreign applications:

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached? YES	NO
092137361	Taiwan R.O.C	12/30/2003	☐	☑	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐

中華民國經濟部智慧財產局

INTELLECTUAL PROPERTY OFFICE
MINISTRY OF ECONOMIC AFFAIRS
REPUBLIC OF CHINA

茲證明所附文件，係本局存檔中原申請案的副本，正確無訛，
其申請資料如下 ：

This is to certify that annexed is a true copy from the records of this office of the application as originally filed which is identified hereunder :

申　　請　　日 ： 西元 2003 年 12 月 30 日
Application Date

申　請　案　號 ： 092137361
Application No.

申　　請　　人 ： 威達電股份有限公司
Applicant(s)

局　　長
Director General

蔡練生

發文日期： 西元 2004 年 3 月 1 日
Issue Date

發文字號：
Serial No. 09320295120

申請日期：	IPC分類
申請案號：	

(以上各欄由本局填註)

發明專利說明書

一、發明名稱	中 文	安全閘道器之加/解密模組動態更新系統及方法
	英 文	A system for actively updating crypt modular in security gateway and method thereof
二、發明人(共2人)	姓 名(中文)	1. 呂致中 2. 曾宏偉
	姓 名(英文)	1. LU CHIH-CHUNG 2. TZENG, HON-WEI
	國 籍(中英文)	1. 中華民國 TW 2. 中華民國 TW
	住居所(中 文)	1. 台北市105敦化北路145巷18號2樓 2. 雲林縣莿桐鄉興北路10之10號
	住居所(英 文)	1. 2.
三、申請人(共1人)	名稱或姓 名(中文)	1. 威達電股份有限公司
	名稱或姓 名(英文)	1. ICP electronic Inc.
	國 籍(中英文)	1. 中華民國 TW
	住居所(營業所)(中 文)	1. 台北縣221汐止市中興路22號3樓 (本地址與前向貴局申請者相同)
	住居所(營業所)(英 文)	1. 3F, NO. 22, Chung-Hsing Rd., Shi-Chi City, Taipei Hsien, 221, Taiwan, R. O. C.
	代表人(中文)	1. 郭博達
	代表人(英文)	1.

四、中文發明摘要　（發明名稱：安全閘道器之加/解密模組動態更新系統及方法）

一種安全閘道器之加/解密模組動態更新系統及方法，係適用於該安全閘道器中，且該安全閘道器如一符合IPSEC通訊協定之虛擬私有網路閘道器，並連接於至少一使用端電腦系統與一網路系統之間。前述加/解密模組動態更新系統至少包括：一網路使用者介面、一模組動態更新單元、一自定模組單元及一延伸函式庫。藉由該網路使用者介面及模組動態更新單元，可讓使用者可輕易地單純更新或新增該閘道器之延伸函式庫內的加/解密碼模組，而無需再連同整個核心碼韌體一起更新，故能節省裝設時間、提昇操作效率，並降低維護成本，且能提昇安全閘道器之加/解密碼模組的可擴充性，使網路傳輸更安全。

五、英文發明摘要　（發明名稱：A system for actively updating crypt modular in security gateway and method thereof）

六、指定代表圖

（一）、本案代表圖為：第____4____圖

（二）、本案代表圖之元件代表符號簡單說明：

104	安全閘道器	110	加/解密模組動態更新系統
114	網路使用者介面	124	工作函式庫
126	模組動態更新單元	128	自定模組單元
134	延伸函式庫	144	延伸函式庫介面
154	組態設定單元	164	核心作業程式
134	延伸函式庫	144	延伸函式庫介面
174	工作排程		

一、本案已向

國家(地區)申請專利	申請日期	案號	主張專利法第二十四條第一項優先權
無			

二、□主張專利法第二十五條之一第一項優先權:

申請案號:

無

日期:

三、主張本案係符合專利法第二十條第一項□第一款但書或□第二款但書規定之期間

日期:

四、□有關微生物已寄存於國外:

寄存國家:

寄存機構: 無

寄存日期:

寄存號碼:

□有關微生物已寄存於國內(本局所指定之寄存機構):

寄存機構:

寄存日期: 無

寄存號碼:

□熟習該項技術者易於獲得,不須寄存。

五、發明說明（1）

【發明所屬之技術領域】

本發明為一種加/解密模組更新系統及方法，特別是一種可運用於安全閘道器之加/解密模組動態更新系統及方法。

【先前技術】

目前市面上最熱門的安全閘道器是一種稱為「虛擬私有網路閘道器」（Virtual Private Network Gateway, VPN Gateway），其中所謂的「虛擬私有網路」係供使用者可在全球任何一遠端地點進入公眾網路環境如網際網路（Internet）或非同步傳輸(ATM)網路，但就使用環境上如同是進入公司內部之區域網路如Intranet或Extranet一樣，故能同時兼顧公眾網路的便利性及內部網路的安全性。正因為如此，利用此類虛擬私有網路，經授權的遠端使用者可藉由連結網際網路與其他使用者、公司、分支機構、經銷商、客戶群建立專屬的連結通道，以傳遞彼此之間重要的訊息。如本發明圖式第1圖，即顯示一種常見的虛擬私有網路架構，其中數個分散於遠端的使用端電腦系統10, 30及40(可位於一區域網路中)利用各自配置之虛擬私有網路閘道器104, 304, 404經由一網際網路50建立起VPN通道602，以彼此傳送重要的資料。當其中任一遠端的使用端電腦系統10, 30及40欲自外部進入公司內部電腦系統如一伺服器電腦系統20時，同樣可利用各自所屬的虛擬私有網路閘道器104, 304, 404建立VPN通道以進行遠端資料存取(Remote Data Access)。

五、發明說明 (2)

前述虛擬私有網路(VPN)之原理係利用一種通道技術(Tunneling)，其採用常見的IPSEC、PPTP、L2TP等三種通訊協定其中之一，在公眾網路如網際網路中構築出一條如同使用在內部網路環境中的安全通道，並以包裝形式(Encapsulation)保護使用端傳送之私密資料的資料封包(Packet)，防止在傳送資料予接收端的過程中遭外人如駭客入侵竊取，同時該私密資料的傳送還可配合其他機制如安全認證、身分辨識(ID Authentication)或加/解密機制(Decryption/Encryption)等，故使該VPN閘道器之功能更趨於多樣化、安全性高及完整。

前述虛擬私有網路之加/解密機制大多以下兩種編碼型式：一種為呈對稱式的密鑰編碼(Secret key cryptography)；以及另一種非對稱式的公鑰編碼(Public key cryptography)。例如在前述IPSEC 通訊協定中，即使用一種網路金鑰交換(Internet key exchange, IKE)協定，其包括在網路金鑰交換型態1及2 (IKE Phases 1 & 2)過程中，產生一公鑰保護一密鑰傳予該接收端，以使該接收端使用該密鑰解開隨後傳來的加密資料。該網路金鑰交換(IKE)協定的用途在於建立、認證及交換一安全參數索引(Security Association, SA)，以辨識資料雙方之身份、溝通要共用的加/解密演算法、以及彼此產生、交換、和建立金鑰。關於建立虛擬私有網路(VPN)之金鑰長度、加/解密演算型態、及加/解密執行函式等描述結構皆記錄在每一台VPN閘道器之一加/解密模組中。

五、發明說明 (3)

惟，雖然目前大部份VPN閘道器製造廠商多有提供各自設計並符合業界標準的加/解密模組，如符合前述IPSEC通訊協定的加/解密模組。然而，為考量到整體系統的安全性、穩定性、執行效率、以及互通性問題，此類加/解密模組的更新機制往往與整個VPN閘道器的核心碼韌體(kernel firmware)的更新機制結合在一起，亦即當只有加/解密模組需要改版或更新時，仍然必須先將整個核心碼韌體一起更新。目前已知的更新方式如本發明圖示第3圖所示，首先進行步驟S200，即一使用端電腦系統(如第1圖所示編碼10)經由其網路瀏覽器(Browser)、網際網路連線至VPN閘道器廠商的伺服器端電腦系統之網站(如第1圖所示編碼20)；步驟S210，開始下載整個新的核心碼韌體至該使用端電腦系統之儲存裝置(如第1圖所示編碼102)中；然後步驟220及S230，再透過VPN閘道器104' 本身之使用者介面(GUI) 114' (見第2圖)上傳該新的核心碼韌體至閘道器 104' 中；步驟S240，利用VPN閘道器 104' 之工作函式庫124'中的核心更新模組 126' (見第2圖)以新的核心碼韌體開始更新其核心作業程式134'；接著步驟S250，在核心更新模組 126' 更新核心碼韌體的過程中，包括在工作函式庫124'中更新其加/解密模組128' (見第2圖)；之後如步驟S260，重新啟動(Rebooting) VPN閘道器104' ，即可達成步驟S270所示，完成新的加/解密模組的更新工作。

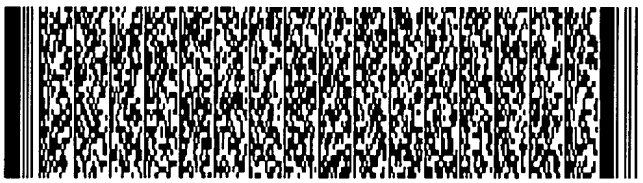
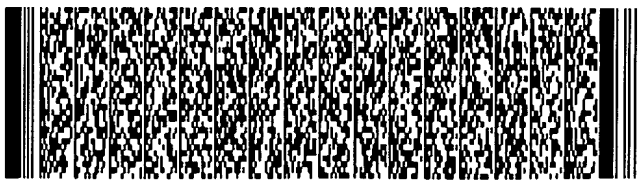
是以，前述習知技術具有下列數個缺點：

（1）雖然每個加/解密碼模組只是佔整個VPN閘道器中極小部分的程式碼之一，但對VPN閘道器而言，該加/解密碼模組所提供的安全性功能極為重要，不能缺少；可是每一VPN閘道器廠商所提供的加/解密碼模組又未必能涵蓋或滿足所有使用者的需求。就目前習知的做法，台VPN閘道器出廠時之原始組態設定即是將加/解密模組永久固定放置於VPN閘道器之工作函式庫(Current Library)中，因此使用者如果要使用到不同的加/解密模組，勢必每次要將整個機器的核心碼韌體一起下載更新，且如此一來廠商為了因應使用上的各種可能性需求，就必須準備包含各種不同組合版本的加/解密模組的核心碼韌體，如此不但下載費時、沒有效率且欠缺彈性，亦容易發生錯誤；對廠商維護產品的版本而言，成本也過高。

（2）習知技術欠缺目前所需要的一種功能，即VPN產品的使用者可依其需要自行開發及裝設屬於他們自己的加/解密模組，而非一定要使用業界的標準模組或廠商提供的標準模組。是以，如果該VPN閘道器產品可以提供方法，讓使用者自行更新或新增加/解密模組，如此彈性的設計可以說是大大地增加了潛在的客戶群，且也可大幅提升VPN閘道器對加/解密碼模組的擴充性。

【發明內容】

為解決前述習知技術之缺點，本發明之一主要目的在於提供一種安全閘道器之加/解密模組動態更新系統及方法，係透過一模組動態更新單元，可讓該閘道器之使用者

每次僅需單純地更新該閘道器之延伸函式庫 (Extended library) 中的加/解密碼模組，而無需再連同整個核心碼韌體一起更新，藉此能節省裝設時間、提昇操作效率，並降低維護成本。

其次，本發明之另一目的在於提供一種安全閘道器之加/解密模組動態更新系統及方法，係透過一自定模組單元及一模組動態更新單元，方便讓該閘道器的使用者自定所需的加/解密碼模組，並將新增之自定加/解密模組置於一延伸函式庫 (Extended library) 中，方便供日後修改更新，藉以提昇安全閘道器之加/解密碼模組的可擴充性，使網路傳輸更安全。

且，本發明之再一目的在於提供一種安全閘道器之加/解密模組動態更新系統及方法，係透過一網路使用者介面(Web GUI)，方便該安全閘道器的使用者在視窗(Window)上輕易選擇所需要的加/解密碼模組，以將新增或更新之密碼模組置於延伸函式庫 (Extended library) 中，故能兼顧操作的方便性及系統運作的效率。

為達到上述發明目的，依據本發明之一種安全閘道器之加/解密模組動態更新系統，係裝設於該安全閘道器中，且該安全閘道器如一符合IPSEC通訊協定之虛擬私有網路閘道器，其具有一工作函式庫、一核心作業程式(Kernel)，以及一工作排程單元，並連接於至少一使用端電腦系統與一網路系統之間。

前述加/解密模組動態更新系統包括：一網路使用者介面、一模組動態更新單元、一自定模組單元、一延伸函式庫、一延伸函式庫介面及一組態設定單元。其中該網路使用者介面，可在該使用端電腦系統產生至少一具有加/解密模組動態更新機制之視窗畫面，以供使用者經此介面依需要選擇性上傳一新版的加/解密模組至該安全閘道器中。該模組動態更新單元，係設於該工作函式庫中，其依據上傳至該安全閘道器的新版加/解密模組的型態，動態更新一延伸函式庫中相對應的現有加/解密模組或新增此上傳的加/解密模組至該延伸函式庫中存放。該延伸函式庫，用於收容前述加/解密模組。該延伸函式庫介面，係輔助前述該延伸函式庫分別與該工作函式庫、核心作業程式作資料溝通。以及該組態設定單元，為一種系統檔，用於設定符合IPSEC通訊協定的執行流程，故當一加/解密模組進行更新或新增后，其現有的網路金鑰交換(IKE)之金鑰交換流程也會接著更新。

此外，依據本發明之一種安全閘道器之加/解密模組動態更新系統，係適用於該安全閘道器中，且該安全閘道器係連接於至少一使用端電腦系統與一網路系統之間，前述加/解密模組動態更新方法至少包括：

使用者自該使用端電腦系統之網路瀏覽器經此網路系統連線至閘道器廠商之網站，以下載一新版的加/解密模組之程式碼至該使用端電腦系統中；

啟動該安全閘道器之一網路使用者介面，以在該使用

端電腦系統上產生至少一具有加/解密模組動態更新機制之視窗畫面；

自該網路使用者介面提供的視窗畫面中，選擇要上傳的新版加/解密模組如增加一自定的加/解密模組；

將所選的新版加/解密模組上傳至至該安全閘道器中；

使安全閘道器之一模組動態更新單元依據該上傳的加/解密模組之類型，動態更新一延伸函式庫中相對應的現有加/解密模組或新增此上傳的加/解密模組至該延伸函式庫中存放；

更新安全閘道器之網路金鑰交換(IKE)協定之金鑰交換流程；以及

使該安全閘道器重新開機以執行更新過後的金鑰交換流程。

【實施方式】

首先請見第4圖，為依據本發明之較佳實施例之一種安全閘道器之加/解密模組動態更新系統110，其裝設於一網路安全閘道器104中，且該安全閘道器104如第1圖所示，可為一連接網際網路50之虛擬私有網路閘道器(VPN Gateway)，其符合IPSEC通訊協定，以供一使用端電腦系統10建立一虛擬私有網路通道來安全傳遞私密資料予其他使用端電腦系統30及40。此外，該安全閘道器104至少具有一工作函式庫(Current Library)124，其內可設置有一固定(default)的加/解密模組A、一核心作業程式

(Kernel)164 為該安全閘道器104的作業系統，以及一工作排程單元(Daemon) 174，用於依序安排整個閘道器需要處理的工作如儲存資料、發送資料、更新加/解密模組等。

前述加/解密模組動態更新系統110至少包括：一網路使用者介面114、一模組動態更新單元126、一自定模組單元128、一延伸函式庫134、一延伸函式庫介面144及一組態設定單元154。其中該網路使用者介面114，係在該使用端電腦系統10上產生至少一具有複數個加/解密模組動態更新機制之視窗畫面，以方便使用者輕易操作或設定該安全閘道器104，如其中一機制，提供更新該安全閘道器104中現有的加/解密模組，或如另一機制，提供使用者可以額外新增一組自定的加/解密模組至該安全閘道器104中存放。當然，使用者在啟動該網路使用者介面114以進行安全閘道器104之加/解密模組更新前，一樣必須先經網際網路連線至該安全閘道器廠商的網站(如第1圖所示編碼20)，但僅需下載一新的加/解密模組的程式碼至該使用端電腦系統中即可，故不同於習知技術需要每次下載全部核心碼韌體。

該模組動態更新單元126係裝設於該安全閘道器104之工作函式庫(Current Library)124中，並依據使用者自前述網路使用者介面114上傳的一加/解密模組類型，動態更新或新增此加/解密模組至該延伸函式庫134中存放。是以，該延伸函式庫134中可以同時放置數組加/解密模組，

如一組更新版的加/解密模組B及另一組自定的加/解密模組C。

該自定模組單元128係裝設於該安全閘道器104之工作函式庫(Current Library)124中，並與前述該網路使用者介面114之具自定加/解密模組機制相連接，藉以產生該自定模組單元128之所屬視窗畫面(未顯示)，以方便使用者依據此畫面指示，依序填入欲自定的加/解密模組之描述結構於該視窗之空白欄位內。這此描述結構包括演算法型態、演算法識別碼、資料加密區塊大小、金鑰長度大小、加/解密執行函式。其中該加/解密執行函式之參數進一步包括資料區塊位址、資料區塊大小、金鑰內容、金鑰長度、初始向量、加解密旗標等。

當該自定模組單元128完成自定的加/解密模組C時，必須同樣透過前述網路使用者介面114上傳自定的加/解密模組C，以供該模組動態更新單元126新增此自定的加/解密模組C至該延伸函式庫134中存放。其中該延伸函式庫介面144，用於輔助前述該延伸函式庫分別與該安全閘道器104之工作函式庫124、核心作業程式164作資料溝通。

該組態設定單元154，如一種系統檔，用於設定符合IPSEC通訊協定的執行流程，故當一加/解密模組進行更新或新增后，其現有的網路金鑰交換(Internet key exchange, IKE)協定之金鑰交換程序也會接著更新成如下步驟：(1)在每一網路金鑰交換型態1或2(IKE Phase 1 or 2)中皆先判斷該工作函式庫124是否具有固定(Default)的

加/解密模組；(2)如無，則再進一步判斷該延伸函式庫134中是否具有任何新增或更新的加/解密模組，直到選擇出一組加/解密模組的金鑰進行交換；以及(3)當該網路金鑰交換型態(IKE)完成所有的金鑰交換流程之後，接著通知網路核心(kernel)164進行現有IPSEC協定的安全參數索引(SA)更新。

此外，請見第5圖為依據本發明之較佳實施例之一種安全閘道器之加/解密模組動態更新方法，其步驟包括：

首先進行步驟S300，自一使用端電腦系統(如第1圖所示編碼10)之網路瀏覽器(Browser)經由網際網路連線至安全閘道器廠商所屬伺服器端電腦系統之網站(如第1圖所示編碼20)；

步驟S302，開始下載新版的加/解密模組至該使用端電腦系統之儲存裝置(如第1圖所示編碼102)中；

步驟S304，使用者啟動安全閘道器104之網路使用者介面(GUI)114；

步驟S306，使用者自該網路使用者介面(GUI)114所提供的視窗畫面中選擇要上傳的加/解密模組。若使用者選擇自定加/解密模組C，則進行步驟S308，即啟動一自定模組單元128的視窗畫面，以供使用者開始依該畫面指示輸入此自定加/解密模組的描述結構，包括如演算法型態、演算法識別碼、資料加密區塊大小、金鑰長度大小、加/解密執行函式，其中該加/解密執行函式之參數進一步包括資料區塊位址、資料區塊大小、金鑰內容、金鑰長度、

初始向量、加解密旗標等。待使用者確認其輸入的自定加/解密模組C的參數無誤后，進行步驟S310，即上傳此新增的加/解密模組C至安全閘道器104中；反之，若使用者選擇前述步驟S304之更新版加/解密模組B，則在步驟S310中會直接上傳此更新版的加/解密模組B至安全閘道器104中；

步驟S312，使安全閘道器104之模組動態更新單元126判斷該上傳的加/解密模組為更新的加/解密模組或為新增的自定加/解密模組。若判斷結果為更新的加/解密模組，則進行步驟S316，對延伸函式庫134中相對應的先前版加/解密模組進行更新；反之，若判斷結果為自定的加/解密模組，則進行步驟S314，即將此自定的加/解密模組放置於該延伸函式庫134中；

接著步驟S317，更新安全閘道器104之組態設定單元154中有關網路金鑰交換(IKE)協定之金鑰交換流程（待后詳述）；

接著步驟S318，重新啟動(Rebooting)此安全閘道器104，使該安全閘道器104執行更新過後的金鑰交換流程；以及

最後步驟S320，即完成加/解密模組的更新工作。

請進一步見第6圖，係依據第5圖步驟S318之一經更新過后的網路金鑰交換(IKE)協定之金鑰交換流程方法，其運用於一接收端及一發出端(如第1圖所示之使用端電腦系統10及30)之間有關私密資料傳送的先期溝通，其步驟包

括：

步驟S400，安全閘道器104之現有IPSEC安全參數索引(IPSEC SA)進行初始化；

步驟S410，進行網路金鑰交換型態1(IKE Phase 1)；

步驟S420，判斷該工作函式庫124中是否存在一適當加/解密模組，如一固定(Default)的加/解密模組。如果是，則進行步驟S430，即選用該固定的加/解密模組的金鑰及運算邏輯來與對方如接收端溝通；反之，若在工作函式庫124未發現任何一組可被接受的加/解密模組時，則進行步驟S422，即進一步判斷該延伸函式庫134中是否存在一組適當加/解密模組，如一新增或更新的加/解密模組。如果是，則進行步驟S430，即選用該新增或更新的加/解密模組來與對方如接收端溝通；

接著步驟S440，進行網路金鑰交換型態2(IKE Phase 2)；

步驟S450、S455及S460分別重覆前述步驟S420、S422至S430之相同動作。倘若在步驟S422或S455中未發現任何適當的加/解密模組，則進行至步驟S462，即系統產生一錯誤訊息；

最後步驟S470，完成該網路金鑰交換型態1及2之所有的金鑰交換流程；以及

接著步驟S480，通知該安全閘道器104之網路核心(kernel)164以更新現有IPSEC協定的安全參數索引(SA)。基於前述，可知依據本發明之安全閘道器之加/解密模組

動態更新系統及方法，係透過一模組動態更新單元，使該閘道器之使用者每次僅需單純地更新或新增該閘道器之延伸函式庫的加/解密碼模組，而無需再同如習知技術將整個核心碼韌體一起更新，故能節省裝設時間、提昇操作效率，並降低廠商維護產品的版本。此外，依據本發明之自定模組單元及使用者介面(GUI)，可方便讓使用者自定所需的加/解密碼模組，藉此可提昇安全閘道器之加/解密碼模組的可擴充性。

雖然本發明已以較佳實施例揭露如上，然其並非用以限定本發明，任何熟悉此項技藝者，在不脫離本發明之精神和範圍內，當可做些許更動與潤飾，因此本發明之保護範圍當視後附之申請專利範圍所界定者為準。

圖式簡單說明

為使本發明之上述目的、特徵和優點能更明顯易懂，下文特舉實施例，並配合所附圖示，詳細說明如下：

第1圖係顯示依據本發明較佳實施例之一種安全閘道器運用於一網路系統上之架構；

第2圖係顯示一具加/解密模組之習知安全閘道器結構；

第3圖係顯示依據前述第2圖之習知安全閘道器之加/解密模組之更新流程圖；

第4圖係顯示依據本發明較佳實施例之安全閘道器之加/解密模組動態更新系統之結構；

第5圖係顯示依據本發明實施例之安全閘道器之加/解密模組動態更新方法之流程圖；以及

第6圖係顯示依據本發明實施例之安全閘道器之網路金鑰交換(IKE)協定之金鑰交換流程之流程圖。

符號說明：

10,30,40	使用端電腦系統
20	伺服器端電腦系統
50	網路系統
102	儲存系統
104,304,404,104'	安全閘道器
110	加/解密模組動態更新系統
114,114'	網路使用者介面
124	工作函式庫

圖式簡單說明

126	模組動態更新單元
128	自定模組單元
134,124'	延伸函式庫
144	延伸函式庫介面
154	組態設定單元
164,134'	核心作業程式
134	延伸函式庫
144	延伸函式庫介面
174,144'	工作排程
602	虛擬私有網路通道
126'	核心更新模組
128'	加/解密模組

S200, S210, S220, S230, S240, S250, S260, S270, S300, S302, S304, S306, S308, S310, S312, S314, S316, S317, S318, S320, S400, S410, S420, S422, S430, S440, S450, S455, S460, S462, S470, S480 為操作步驟

六、申請專利範圍

1. 一種安全閘道器之加/解密模組動態更新系統，且該安全閘道器係連接於一使用端電腦系統與一網路系統之間，前述前述加/解密模組動態更新系統至少包括：

一網路使用者介面，在該使用端電腦系統產生至少一具有加/解密模組動態更新機制之視窗畫面，以供使用者經此介面僅只上傳一新版的加/解密模組至該安全閘道器中；

一模組動態更新單元，係依據上傳該安全閘道器的新版加/解密模組，動態更新一延伸函式庫中相對應的現有加/解密模組或新增此上傳的加/解密模組至該延伸函式庫中存放；以及

該延伸函式庫，用於收容前述加/解密模組。

2. 如申請專利範圍第1項所述之加/解密模組動態更新系統，其中該安全閘道器為一符合IPSEC通訊協定之虛擬私有網路閘道器(VPN Gateway)。

3. 如申請專利範圍第1項所述之加/解密模組動態更新系統，其中該安全閘道器至少具有一工作函式庫(Current Library)、一核心作業程式(Kernel)，以及一工作排程單元(Daemon)，其中前述模組動態更新單元即位於該工作函式庫中。

4. 如申請專利範圍第1項所述之加/解密模組動態更新系統，其中該網路使用者介面之視窗畫面之加/解密模組動態更新機制更包括一機制，可提供使用者更新該安全閘道器中現有的加/解密模組。

六、申請專利範圍

5. 如申請專利範圍第4項所述之加/解密模組動態更新系統，其中該網路使用者介面之視窗畫面之加/解密模組動態更新機制更包括另一機制，可提供使用者新增一組自定的加/解密模組至該安全閘道器中存放。

6. 如申請專利範圍第5項所述之加/解密模組動態更新系統，進一步包括一自定模組單元，與前述網路使用者介面之自定加/解密模組機制相連結，藉以產生一所屬視窗畫面，供使用者依此畫面指示填入欲自定的加/解密模組之描述結構。

7. 如申請專利範圍第6項所述之加/解密模組動態更新系統，其中前述自定加/解密模組之描述結構至少包括：演算法型態、演算法識別碼、資料加密區塊大小、金鑰長度大小及加/解密執行函式，其中該加/解密執行函式之參數進一步包括資料區塊位址、資料區塊大小、金鑰內容、金鑰長度、初始向量、加解密旗標等。

8. 如申請專利範圍第1項所述之加/解密模組動態更新系統，其中該模組動態更新單元，係依據此新版加/解密模組之類型，選擇動態更新一延伸函式庫中相對應的現有加/解密模組或新增此上傳的加/解密模組至該延伸函式庫中存放。

9. 如申請專利範圍第2項所述之加/解密模組動態更新系統，進一步具有一延伸函式庫介面，係輔助前述該延伸函式庫分別與該工作函式庫、核心作業程式作資料溝通。

10. 如申請專利範圍第1項所述之加/解密模組動態更新系

統，進一步具有一組態設定單元，為一種系統檔，用於設定符合IPSEC通訊協定的執行流程，故當一加/解密模組進行更新或新增后，其現有的網路金鑰交換(IKE)之金鑰交換程序也會接著更新。

11. 一種安全閘道器之加/解密模組動態更新方法，且該安全閘道器係連接於一使用端電腦系統與一網路系統之間，前述加/解密模組動態更新方法至少包括：

自該使用端電腦系統經此網路系統下載一新版的加/解密模組至該使用端電腦系統中；

啟動該安全閘道器之一網路使用者介面，以在該使用端電腦系統上產生至少一具有加/解密模組動態更新機制之視窗畫面；

自該網路使用者介面提供的視窗畫面中，選擇要上傳的新版加/解密模組；

將所選的新版加/解密模組上傳至至該安全閘道器中；

使安全閘道器之一模組動態更新單元依據該上傳的加/解密模組之類型，動態更新一延伸函式庫中相對應的現有加/解密模組或新增此上傳的加/解密模組至該延伸函式庫中存放；以及

更新安全閘道器之網路金鑰交換(IKE)協定之金鑰交換流程；

12. 如申請專利範圍第11項所述之加/解密模組動態更新方法，其中該網路使用者介面之視窗畫面之加/解密模組動

態更新機制更包括一機制，可提供使用者更新該安全閘道器中現有的加/解密模組。

13. 如申請專利範圍第12項所述之加/解密模組動態更新方法，其中該網路使用者介面之視窗畫面之加/解密模組動態更新機制更包括另一機制，可提供使用者新增一組自定的加/解密模組至該安全閘道器中存放。

14. 如申請專利範圍第13項所述之加/解密模組動態更新方法，進一步包括：當前述自定的加/解密模組機制被啟動時，會產生一視窗畫面供使用者依此畫面指示填入欲自定的加/解密模組之描述結構。

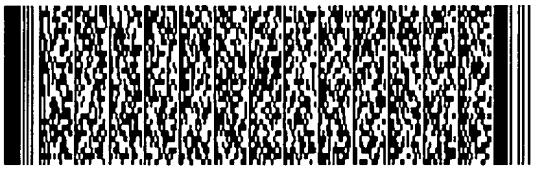
15. 如申請專利範圍第14項所述之加/解密模組動態更新方法，其中前述自定加/解密模組之描述結構至少包括：演算法型態、演算法識別碼、資料加密區塊大小、金鑰長度大小及加/解密執行函式，其中該加/解密執行函式之參數進一步包括資料區塊位址、資料區塊大小、金鑰內容、金鑰長度、初始向量、加解密旗標等。

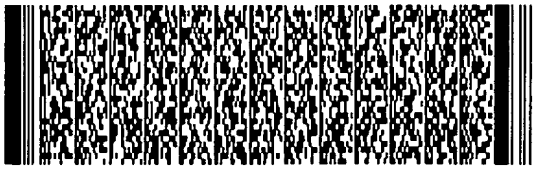
16. 如申請專利範圍第11項所述之加/解密模組動態更新方法，進一步包括:使該安全閘道器執行更新過後的金鑰交換流程。

17. 一種安全閘道器之網路金鑰交換(IKE)協定之金鑰交換流程，包括：

(a)初始化該安全閘道器之現有IPSEC協定之安全參數索引(SA)；

(b)進行網路金鑰交換型態1 (IKE Phase 1)；





六、申請專利範圍

(c)當未在該安全閘道器之工作函式庫中發現一適當的加/解密模組時，進一步自該安全閘道器之一延伸函式庫中取用至少一適當的加/解密模組；

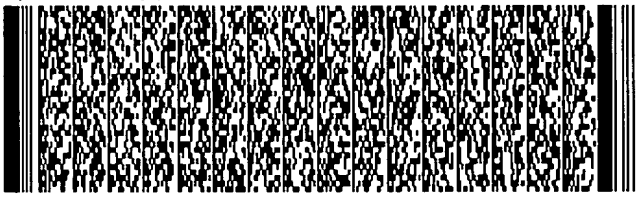
(d)進行網路金鑰交換型態2 (IKE Phase 2)；

(e)重覆前述步驟(c)之相同動作；

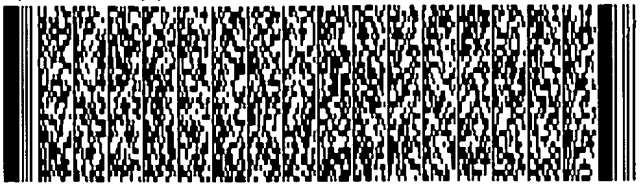
(f)完成網路金鑰交換型態1及2的金鑰交換流程；以及

(g)通知該安全閘道器之網路核心(kernel)進行更新現有IPSEC協定的安全參數索引(SA)。

第 1/24 頁



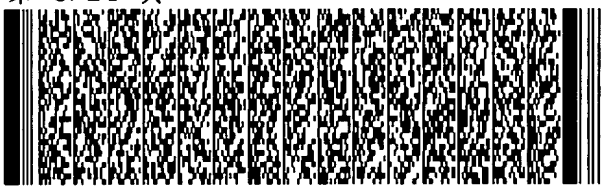
第 2/24 頁



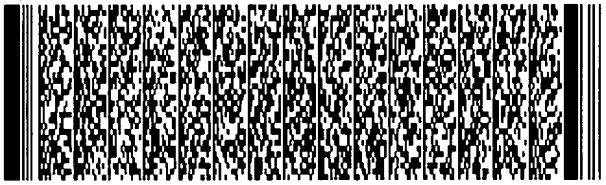
第 3/24 頁

第 4/24 頁

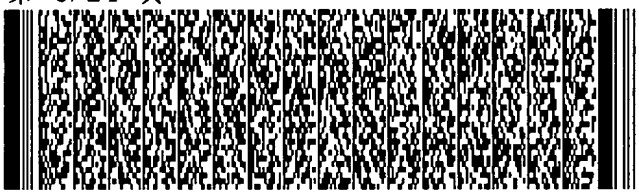
第 5/24 頁



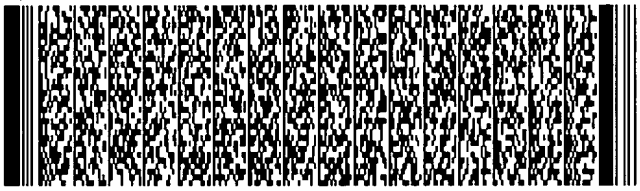
第 5/24 頁



第 6/24 頁

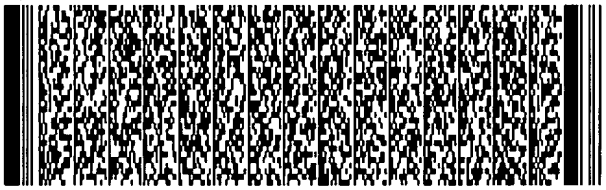


第 6/24 頁

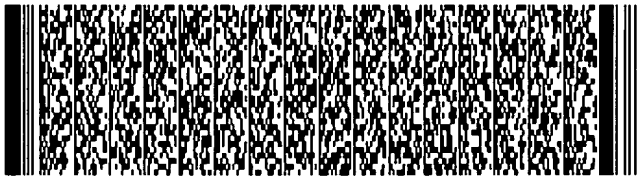


第 7/24 頁

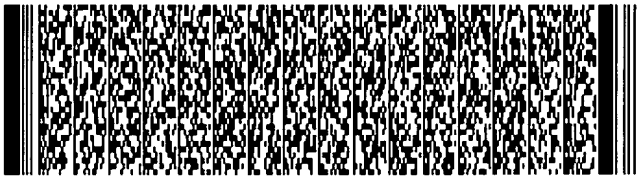
第 7/24 頁



第 8/24 頁

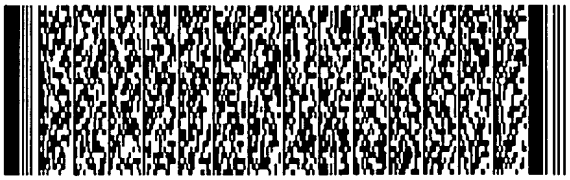


第 8/24 頁

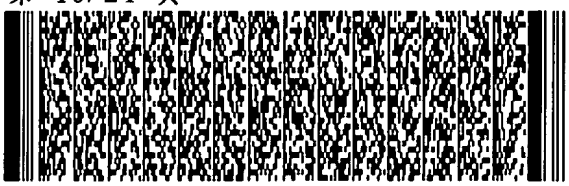


第 9/24 頁

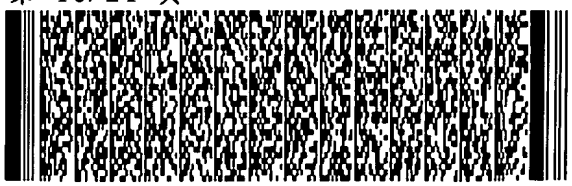
第 9/24 頁



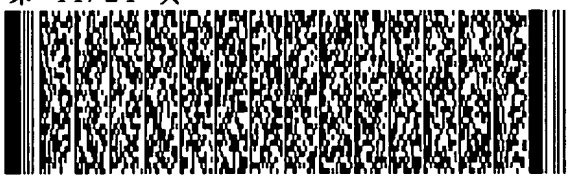
第 10/24 頁



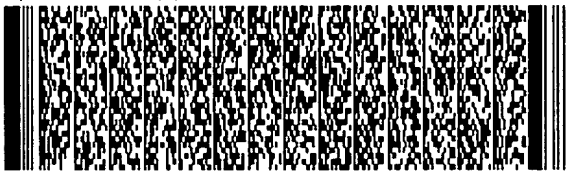
第 10/24 頁



第 11/24 頁

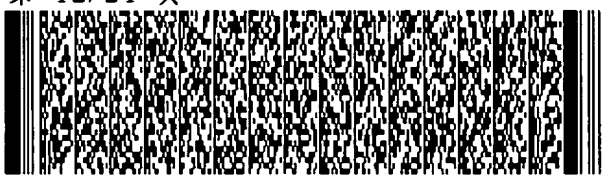


第 11/24 頁



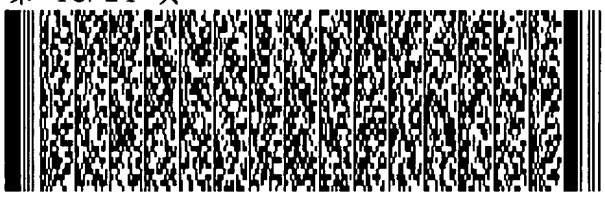
第 12/24 頁

第 12/24 頁

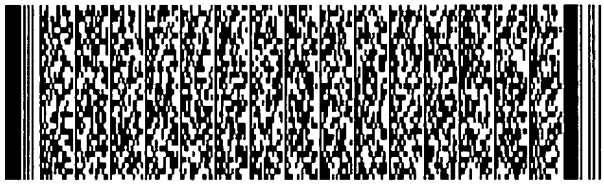


第 13/24 頁

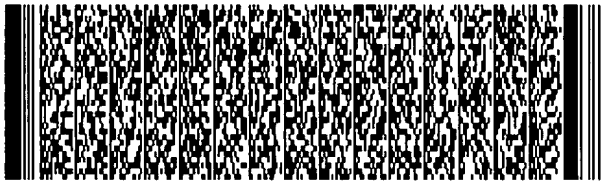
第 13/24 頁



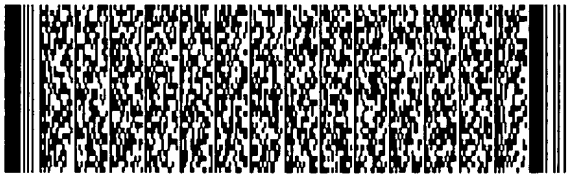
第 14/24 頁



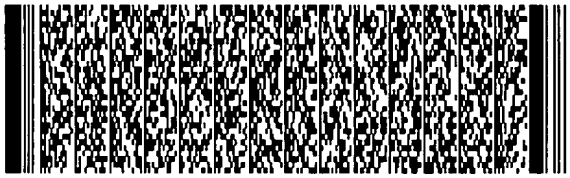
第 14/24 頁



第 15/24 頁



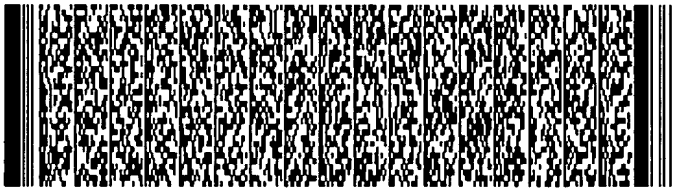
第 15/24 頁



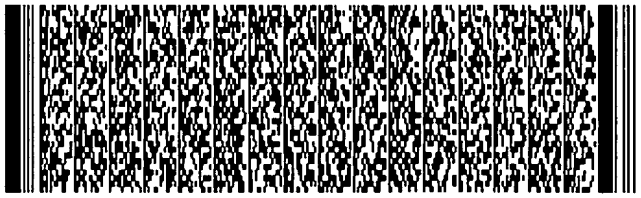
第 16/24 頁

第 16/24 頁

第 17/24 頁

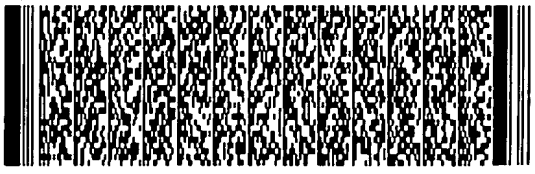


第 18/24 頁

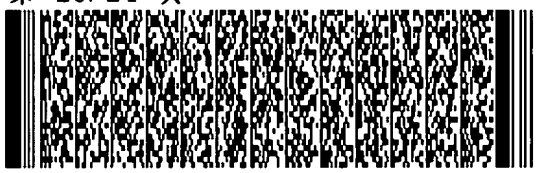


第 19/24 頁

第 20/24 頁



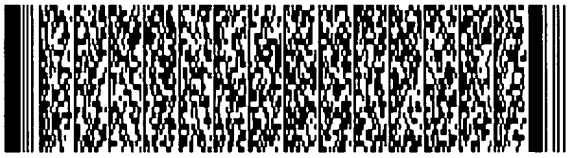
第 20/24 頁



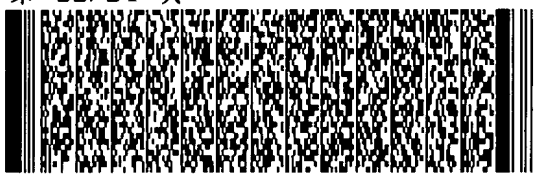
第 21/24 頁

第 21/24 頁

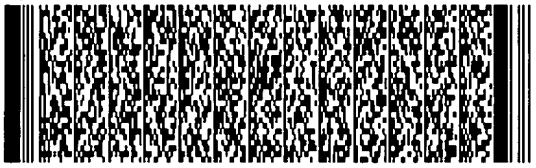
第 22/24 頁



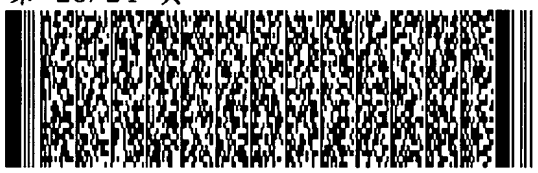
第 22/24 頁



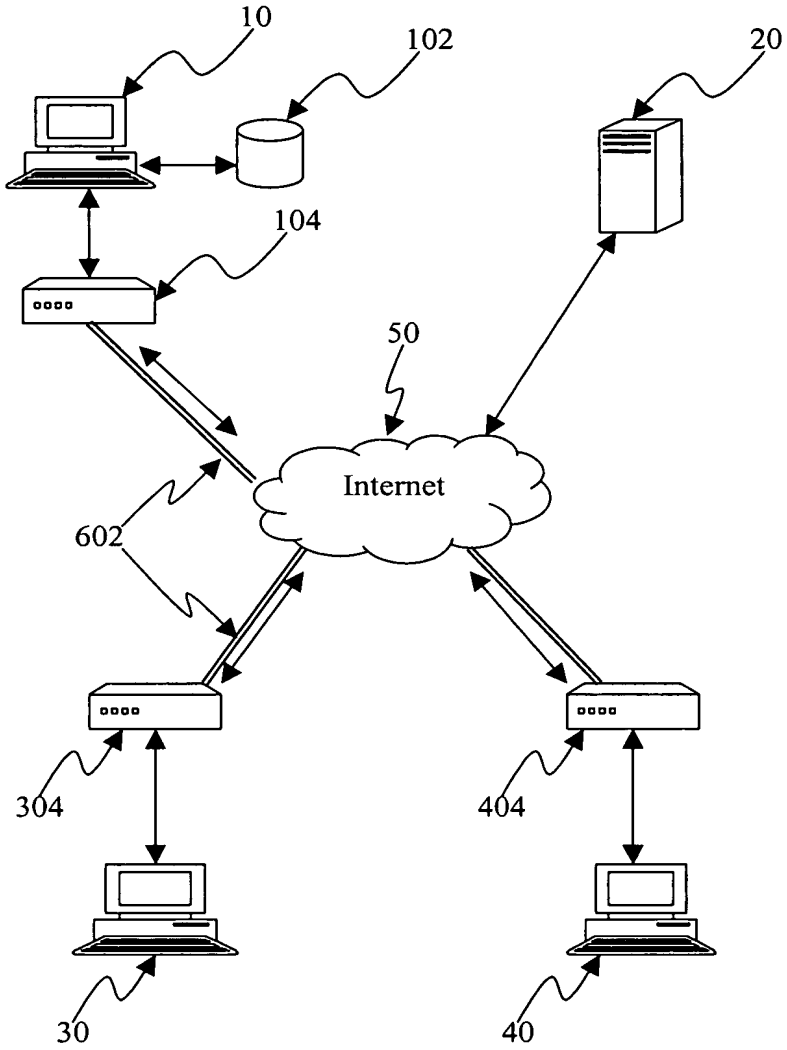
第 23/24 頁



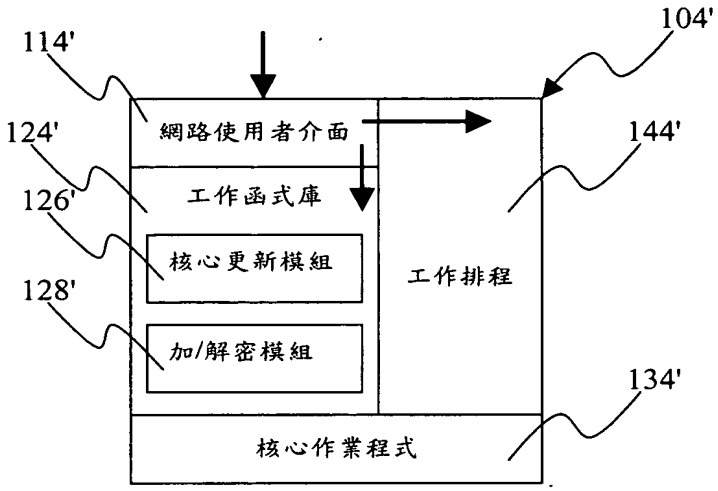
第 23/24 頁



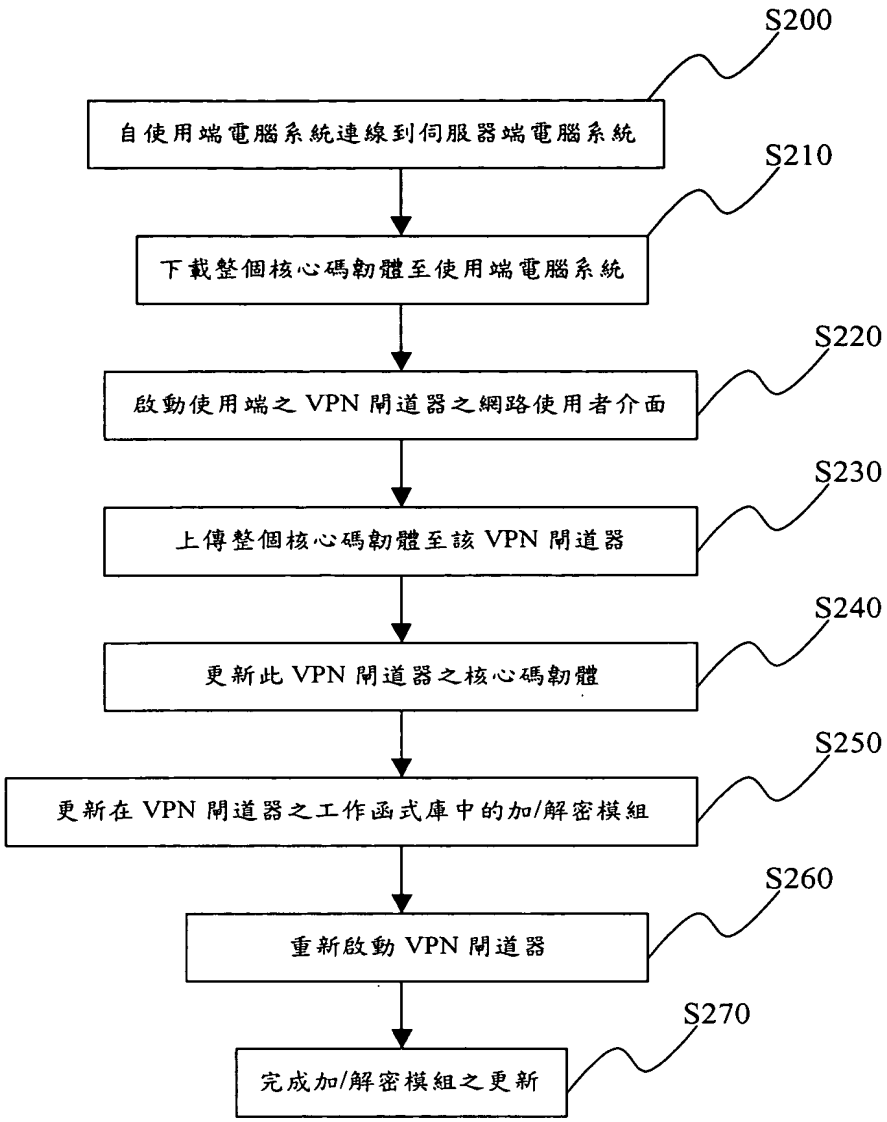
第 24/24 頁



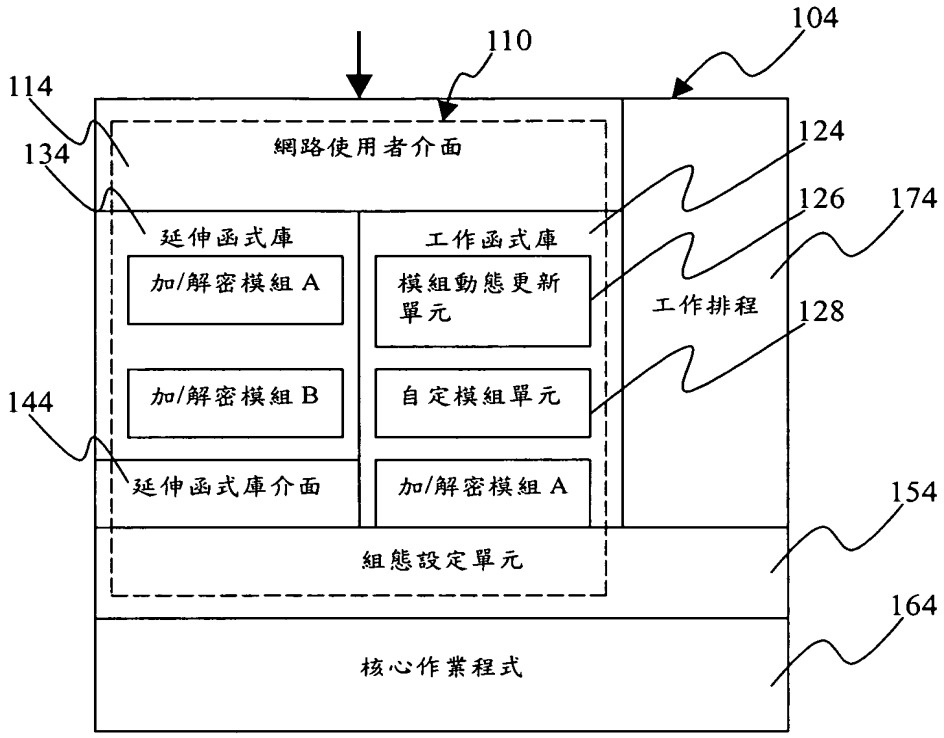
第 1 圖


114'
104'
網路使用者介面
124'
144'
工作函式庫
126'
核心更新模組
工作排程
128'
加/解密模組
134'
核心作業程式

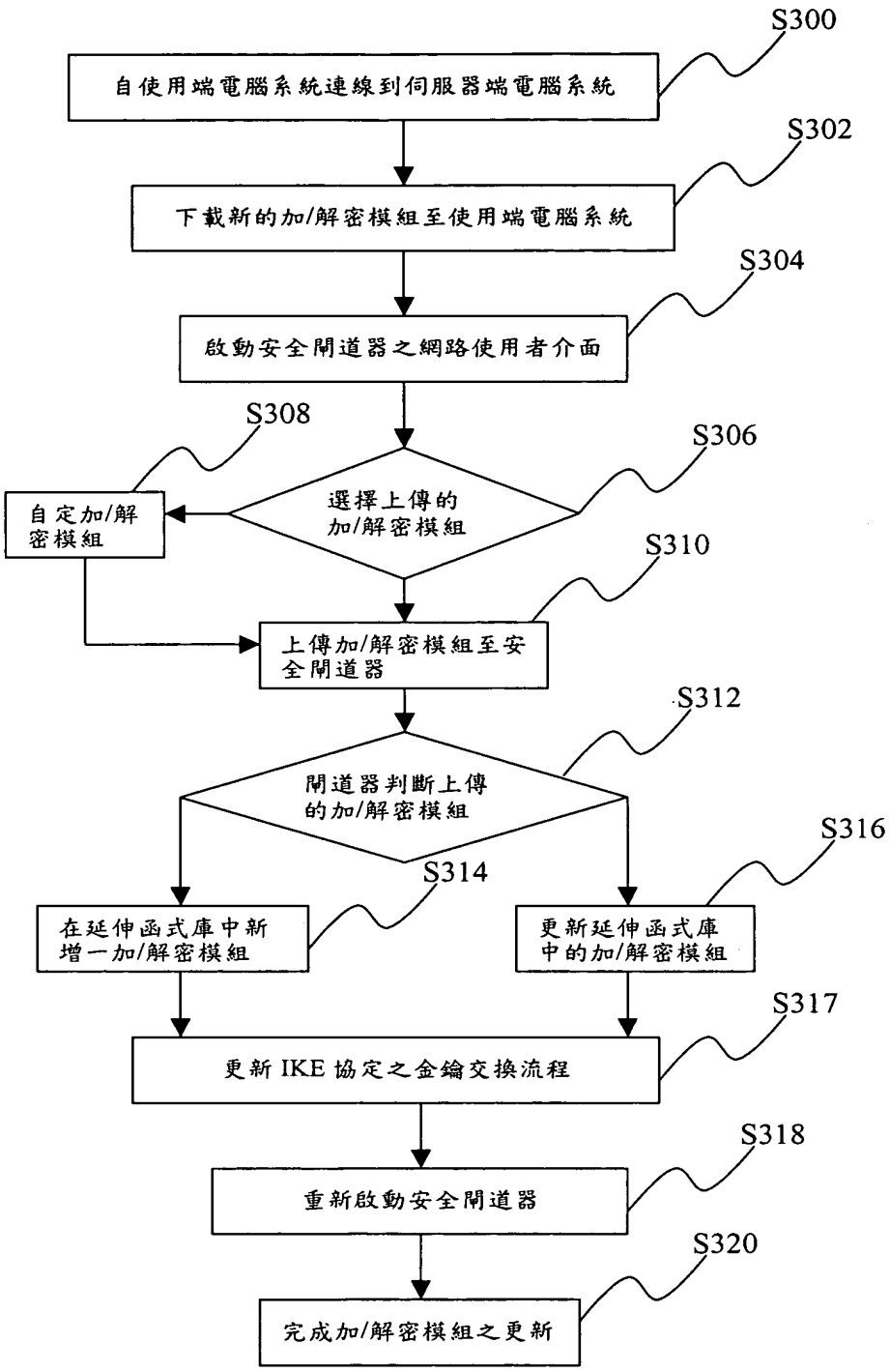
第 2 圖


S200
自使用端電腦系統連線到伺服器端電腦系統
S210
下載整個核心碼韌體至使用端電腦系統
S220
啟動使用端之 VPN 閘道器之網路使用者介面
S230
上傳整個核心碼韌體至該 VPN 閘道器
S240
更新此 VPN 閘道器之核心碼韌體
S250
更新在 VPN 閘道器之工作函式庫中的加/解密模組
S260
重新啟動 VPN 閘道器
S270
完成加/解密模組之更新

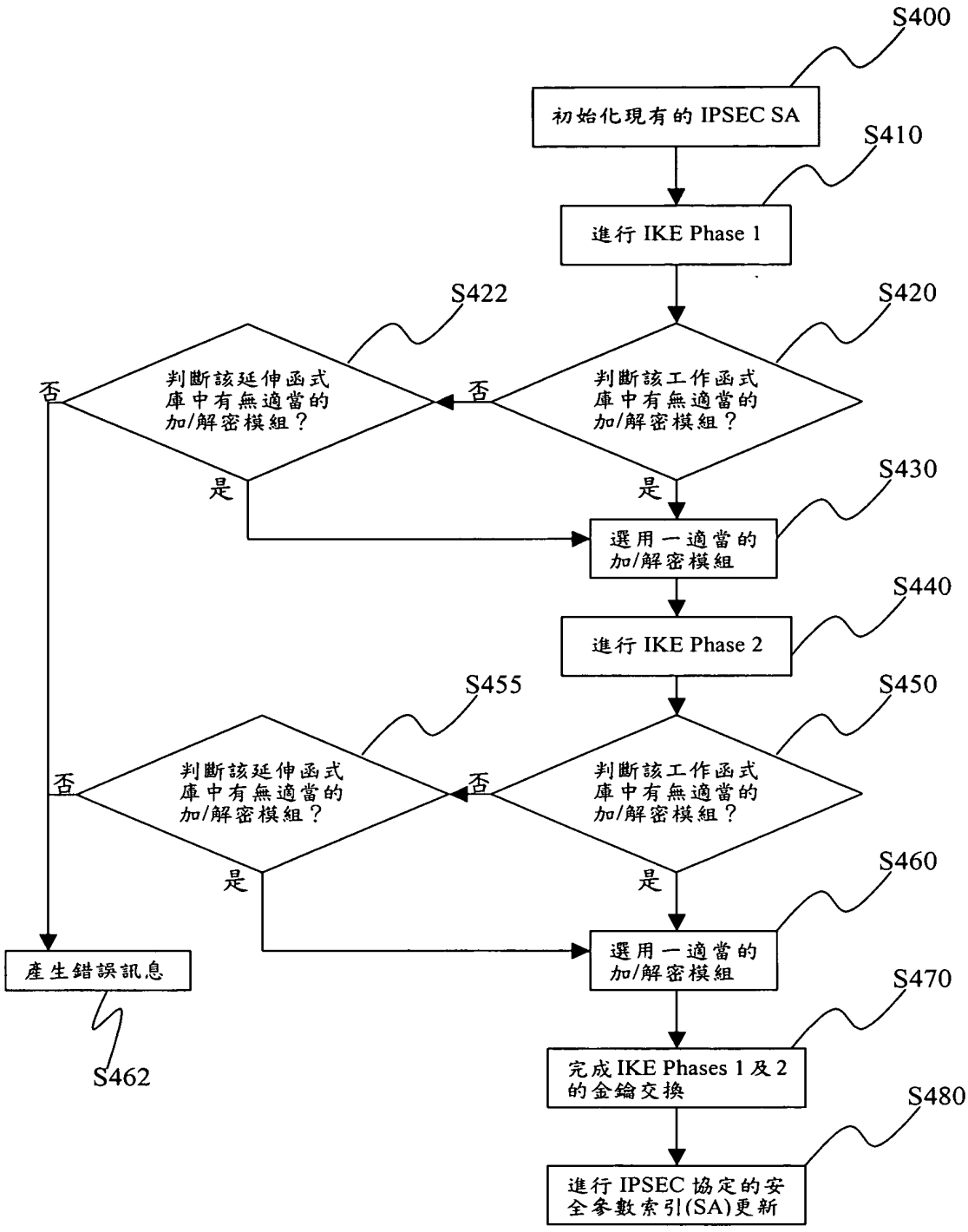
第 3 圖


104
110
114
134
網路使用者介面
124
126
174
延伸函式庫
工作函式庫
加/解密模組 A
模組動態更新單元
工作排程
128
加/解密模組 B
自定模組單元
144
延伸函式庫介面
加/解密模組 A
154
組態設定單元
164
核心作業程式

第 4 圖


S300
自使用端電腦系統連線到伺服器端電腦系統
S302
下載新的加/解密模組至使用端電腦系統
S304
啟動安全閘道器之網路使用者介面
S306
選擇上傳的加/解密模組
S308
自定加/解密模組
S310
上傳加/解密模組至安全閘道器
S312
閘道器判斷上傳的加/解密模組
S314
在延伸函式庫中新增一加/解密模組
S316
更新延伸函式庫中的加/解密模組
S317
更新 IKE 協定之金鑰交換流程
S318
重新啟動安全閘道器
S320
完成加/解密模組之更新

第 5 圖


S400
初始化現有的 IPSEC SA
S410
進行 IKE Phase 1
S422
判斷該延伸函式庫中有無適當的加/解密模組？
否
S420
判斷該工作函式庫中有無適當的加/解密模組？
否
是
是
S430
選用一適當的加/解密模組
S440
進行 IKE Phase 2
S455
判斷該延伸函式庫中有無適當的加/解密模組？
否
S450
判斷該工作函式庫中有無適當的加/解密模組？
否
是
是
S460
選用一適當的加/解密模組
產生錯誤訊息
S462
S470
完成 IKE Phases 1 及 2 的金鑰交換
S480
進行 IPSEC 協定的安全參數索引(SA)更新

第 6 圖